What is claimed is:

1. An apparatus comprising:

one or more cryptographic units; and

a memory to store one or more data encryption keys and an associated header for the one or more data encryption keys, wherein the associated header defines which of the one or more cryptographic units are to use the data encryption key.

2. The apparatus of claim 1, wherein the associated header defines a usage type for the data encryption key.

3. The apparatus of claim 2 further comprising a controller to restrict which of the one more cryptographic units are to use the data encryption key and a type of operation based on the associated header for the data encryption key.

4. The apparatus of claim 1, wherein the associated header defines an identification of a key encryption key used to encrypt the one or more data encryption keys.

5. The apparatus of claim 1, wherein the one or more cryptographic units is from a group consisting of an advanced encryption standard unit, a data encryption standard unit, a message digest unit and a secure hash algorithm unit or an exponential algorithmic unit.

6. An apparatus comprising:

a cryptographic processor within a wireless device, the cryptographic processor comprising:

a first cryptographic unit to generate an intermediate result from execution of a first operation; and

a second cryptographic unit to generate a final result from execution of a second operation based on the intermediate result, wherein the intermediate result is not accessible external to the cryptographic processor.

7. The apparatus of claim 6, wherein the first cryptographic unit and the second cryptographic unit are from a group consisting of an advanced encryption standard unit, a data encryption standard unit, a message digest unit and a secure hash algorithm unit or an exponential algorithmic unit.

8. The apparatus of claim 6, wherein the first operation includes the use of a cryptographic key, wherein the cryptographic key is not loaded into the first cryptographic unit until the cryptographic key is authenticated.

9. A system comprising

a dipole antenna to receive a communication;

an application processor to generate a primitive instruction for a cryptographic operation that is to use a cryptographic key based on the communication; and

a cryptographic processor that comprises:

a memory to store the cryptographic key;

a number of cryptographic units, wherein one of the number of cryptographic units is to generate a challenge to the use of the cryptographic key, wherein the application processor is to generate a response to the challenge; and

a controller to load the cryptographic key into one of the number of cryptographic units for execution of the cryptographic operation if the response is correct.

10. The system of claim 9, wherein the cryptographic processor further comprises a nonvolatile memory that is to store a number of microcode instructions,

wherein the controller is to load the cryptographic key into one of the number of cryptographic units based on at least part of the number of microcode instructions.

11. The system of claim 9, wherein the controller is to abort execution of the cryptographic operation if the response is not correct.

12. The system of claim 9, wherein the response includes a hash of a password associated with the cryptographic key.

13. A system comprising:

an application processor, within a wireless device, to generate a primitive instruction related to a cryptographic operation; and

a cryptographic processor, within the wireless device, the cryptographic processor comprising:

a controller to receive the primitive instruction, wherein the controller is to retrieve a number of microcode instructions from a nonvolatile memory within the cryptographic processor;

a first functional unit to generate an intermediate result from execution of a first operation based on a first of the number of microcode instructions; and

a second functional unit to generate a final result for the cryptographic operation based on the intermediate result, from execution of a second operation based on a second of the number of microcode instructions, wherein the intermediate result is not accessible external to the cryptographic processor.

14. The system of claim 13, wherein the cryptographic processor further comprises a volatile memory to store a cryptographic key.

15. The system of claim 14, wherein the second functional unit is to use the cryptographic key to generate the final result, wherein the controller is not to load the cryptographic key into the second functional unit until the application processor is to authenticate the cryptographic key.

16. A method comprising:

receiving a primitive instruction into a cryptographic processor, for execution of a cryptographic operation that uses a data encryption key that is protected within the cryptographic processor;

retrieving the data encryption key and an associated header for the data encryption key, wherein the associated header defines which of one or more cryptographic units are to use the data encryption key; and

performing an operation within one of the one or more cryptographic units using the data encryption key, if the associated header defines the one of the one or more cryptographic units.

17. The method of claim 16, wherein the associated header defines a usage type for the data encryption key.

18. The method of claim 17, wherein performing the operation within one of the one or more cryptographic units using the data encryption key comprises performing the operation within one of the one or more cryptographic units using the data encryption key if a type of the operation is defined by the usage type.

19. A method comprising:

receiving a primitive instruction into a cryptographic processor from an application executing on an application processor, for execution of a cryptographic operation that uses a cryptographic key that is protected within the cryptographic processor;

generating a challenge for use of the cryptographic key back to the application;

receiving a response to the challenge into the cryptographic processor from the application;

performing the following operations, if the response is correct:

loading the cryptographic key into a functional unit of the cryptographic processor; and

executing an operation within the functional unit using the cryptographic key.

20. The method of claim 19, further comprising aborting execution of the primitive instruction if the response is not correct.

21. The method of claim 19, wherein receiving the response to the challenge into the cryptographic processor from the application includes receiving a hash of a password associated with the cryptographic key.

22. The method of claim 21, wherein performing the following operations, if the response is correct comprises performing the following operations, if the hash of the password is equal to a hash of the password generated within the cryptographic processor.

23. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving a primitive instruction into a cryptographic processor, for execution of a cryptographic operation that uses a data encryption key that is protected within the cryptographic processor;

retrieving the data encryption key and an associated header for the data encryption key, wherein the associated header defines which of one or more cryptographic units are to use the data encryption key; and

performing an operation within one of the one or more cryptographic units using the data encryption key, if the associated header defines the one of the one or more cryptographic units.

24. The machine-readable medium of claim 23, wherein the associated header defines a usage type for the data encryption key.

25. The machine-readable medium of claim 24, wherein performing the operation within one of the one or more cryptographic units using the data encryption key comprises performing the operation within one of the one or more cryptographic units using the data encryption key if a type of the operation is defined by the usage type.

26. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving a primitive instruction into a cryptographic processor from an application executing on an application processor, for execution of a cryptographic operation that uses a cryptographic key that is protected within the cryptographic processor;

generating a challenge for use of the cryptographic key back to the application;

receiving a response to the challenge into the cryptographic processor from the application;

performing the following operations, if the response is correct:

loading the cryptographic key into a functional unit of the cryptographic processor; and

executing an operation within the functional unit using the cryptographic key.

27. The machine-readable medium of claim 26, further comprising aborting execution of the primitive instruction if the response is not correct.

28. The machine-readable medium of claim 26, wherein receiving the response to the challenge into the cryptographic processor from the application includes receiving a hash of a password associated with the cryptographic key.

29. The machine-readable medium of claim 28, wherein performing the following operations, if the response is correct comprises performing the following operations, if the hash of the password is equal to a hash of the password generated within the cryptographic processor.